MIKROTIK

ACADEMY

MTCSE outline

CERTIFIED SECURITY ENGINEER

MIKROTIK MTCSE

Duration:	2 days
Outcomes:	By the end of this training session, the participant will be able to plan and implement appropriate security measures suitable for the network at hand.
Target Audience:	Network engineers and technicians wanting to deploy and maintain secure MikroTik device based networks.
Course prerequisites:	A good working knowledge of TCP/IP Basics is required. You must be MikroTik MTCNA Certified (current or expired certificate is fine) to sit this course.

Title	Objective
Module 1 Introduction	• Attacks, mechanisms and services • The most common threats • RouterOS security deployment • **Module 1 laboratory**
Module 2 Firewall	• Packet flow, firewall chains • Stateful firewall • RAW table • SYN flood mitigation using RAW table • RouterOS default configuration • Best practices for management access • Detecting an attack to critical infrastructure services • Bridge filter • Advanced options in firewall filter • ICMP filtering • **Module 2 laboratory**
Module 3 OSI Layer Attacks	• MNDP attacks and prevention • DHCP: rogue servers, starvation attacks and prevention • TCP SYN attacks and prevention • UDP attacks and prevention • ICMP Smurf attacks and prevention • FTP, telnet and SSH brute-force attacks and prevention • Port scan detection and prevention • **Module 3 laboratory**
Module 4 Cryptography	• Introduction to cryptography and terminology • Encryption methods • Algorithms - symmetric, asymmetric • Public key infrastructure (PKI) • Certificates • Self-signed certificates • Free of charge valid certificates • Using the certificates in RouterOS • **Module 4 laboratory**

Module 5 Securing the Router	• Port knocking • Secure connections (HTTPS, SSH, WinBox) • Default ports for the services • Tunneling through SSH • **Module 5 laboratory**

Module 6 Secure Tunnels	• Introduction to IPsec • L2TP + IPsec • SSTP with certificates • **Module 6 laboratory**